2010-12

Social media integration into state-operated fusion centers and local law enforcement : potential uses and challenges

Fresenko, Victoria L.

Monterey, California. Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

SOCIAL MEDIA INTEGRATION INTO STATE-OPERATED FUSION CENTERS AND LOCAL LAW ENFORCEMENT: POTENTIAL USES AND CHALLENGES

by

Victoria L. Fresenko

December 2010

Thesis Co-Advisors: John Rollins
Richard Bergin

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** December 2010	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Social Media Integration into State-Operated Fusion Centers and Local Law Enforcement: Potential Uses and Challenges			**5. FUNDING NUMBERS**
6. AUTHOR(S) Victoria L. Fresenko			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Number _____N.A._____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

The push by the Obama administration for a more transparent, citizen-centric government has created a new way of thinking among federal, state, and local governments: citizen participation has become a mainstay of newly written policies across the country. The adoption of Web 2.0 technologies, particularly social media, within fusion centers and local law enforcement entities could enable a more expedient exchange of information among fusion centers, law enforcement, and the public. The ability to collect and disseminate information on a real-time basis via fusion centers and law enforcement is key to the overall success of the homeland security mission; it is impossible for the federal government to have sole responsibility for safeguarding the homeland from the confines of Washington, D.C. Because fusion centers and law enforcement agencies are state and local entities, they have the capability to obtain information at a grassroots level and have the advantage of knowing the local environment, including potential targets and vulnerabilities. Social media, if leveraged appropriately, could enhance communication among fusion centers, law enforcement, and private citizens to better detect and deter terrorism. This research explores potential benefits and implementation challenges of integrating social media into fusion center and local law enforcement frameworks.

14. SUBJECT TERMS Fusion center, law enforcement, social media, homeland security, local citizens, Web 2.0			**15. NUMBER OF PAGES** 75
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

SOCIAL MEDIA INTEGRATION INTO STATE-OPERATED FUSION CENTERS AND LOCAL LAW ENFORCEMENT: POTENTIAL USES AND CHALLENGES

Victoria L. Fresenko
Deputy Committee Management Officer, Department of Homeland Security
B.A., Kent State University, 2002
M.A., Kent State University, 2003

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)

from the

NAVAL POSTGRADUATE SCHOOL
December 2010

Author: Victoria L. Fresenko

Approved by: John Rollins
Thesis Co-Advisor

Richard Bergin
Thesis Co-Advisor

Harold A. Trinkunas, PhD
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The push by the Obama administration for a more transparent, citizen-centric government has created a new way of thinking among federal, state, and local governments: citizen participation has become a mainstay of newly written policies across the country. The adoption of Web 2.0 technologies, particularly social media, within fusion centers and local law enforcement entities could enable a more expedient exchange of information among fusion centers, law enforcement, and the public. The ability to collect and disseminate information on a real-time basis via fusion centers and law enforcement is key to the overall success of the homeland security mission; it is impossible for the federal government to have sole responsibility for safeguarding the homeland from the confines of Washington, D.C. Because fusion centers and law enforcement agencies are state and local entities, they have the capability to obtain information at a grassroots level and have the advantage of knowing the local environment, including potential targets and vulnerabilities. Social media, if leveraged appropriately, could enhance communication among fusion centers, law enforcement, and private citizens to better detect and deter terrorism. This research explores potential benefits and implementation challenges of integrating social media into fusion center and local law enforcement frameworks.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

CIA	Central Intelligence Agency
CIO	Chief Information Officer
CRS	Congressional Research Service
DoD	Department of Defense
DHS	Department of Homeland Security
DoJ	Department of Justice
EPIC	Electronic Privacy Information Center
FEMA	Federal Emergency Management Agency
FOIA	Freedom of Information Act
FOUO	For Official Use Only
GAO	Government Accountability Office
GSA	General Services Administration
HSPI	Homeland Security Policy Institute
IACP	International Association of Chiefs of Police
NOC	National Operations Center
OPS	Office of Operations and Coordination and Planning
PII	Personally Identifiable Information
PIA	Privacy Impact Assessment
PIO	Public Information Officer
STIC	Statewide Terrorism and Intelligence Center (STIC)
UDPS	Utah Department of Public Safety
VDEM	Virginia's Department of Emergency Management
WH	The White House

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to thank my bosses, Georgia Abraham and Becca Sharp, for supporting my participation in the NPS CHDS Master's Program and for their constant encouragement. I would not have been able to finish this program without you.

To my fellow classmates from 0903 and 0904—you have become like family to me, and I will greatly miss our discussions, karaoke, laughter, and adventures in Shepherdstown and Monterey. Although 0903 was clearly the brighter group, I found friendship and support (both personally and professionally) in both cohorts that I won't soon forget. I don't think that the Rumsey room will ever be the same without us. Mark Stigler, your ability to see the bigger picture speaks to your leadership capabilities; thank you for your friendship and for your confidence in me and my project. Thanks also to Keith Squires and Aaron Kustermann who, along with Mark, tolerated endless questions and fit my project into their busy schedules.

To my thesis advisors, John Rollins and Richard Bergin, thank you for your endless patience. Richard, there exists no one as responsive or as dedicated to his students' success as you are. You should be sainted.

Lauren Wollman (a.k.a. the Obi Wan Kanobi of the IRB process) and Greta Marlatt (an institution in and of herself)—you are my heroines. You held my hand through months of an IRB approval and provided tireless guidance through a maze of constant and ever-changing reference needs. Thank you for your faith and kindness.

Thanks also to my family and friends who tolerated my absence and stood behind me during another one of my undertakings; I'm so lucky to have you in my life. Dad, thanks for flying to D.C. to drive my cats to Ohio…twice…and thanks to Grandma Donna and Grandpa Warren for watching them while I was in California. Cindy (mon soeur), thank you for your ad hoc edits and for always making me laugh. You are the smartest, most gifted person I know. Phil, thanks for postponing our vacation so I could

travel to the Dominican Republic and take the time I needed to write my thesis. I owe you some beach time!

Lastly, I'd like to dedicate this thesis to my grandma, Pauline Kavel, who participated in the first form of social media: running to the window every time a car door slammed to see what was going on and then commenting to everyone in earshot. Grandma, you are the unknown inventor of the real-time status update, and I love you more than you'll ever know.

I. INTRODUCTION

A. PROBLEM STATEMENT

The Obama administration has championed the use of new technology to promote transparency within the federal government, vowing to involve the American public in its daily operations. A White House blog on "New Technologies and Participation" encourages the public to engage in discussions with the White House, calling social technology an "unprecedented opportunity to connect you to your government in order to obtain information and services and to participate in policymaking." (White House Blog, 2009). The majority of that collaborative effort, which has centered around the development of Web 2.0 applications, has begun to have a resounding impact on the policies of federal, state, and local governments nationwide. According to Webopedia (2010), Web 2.0 is, "the term given to describe a second generation of the World Wide Web that is focused on the ability for people to collaborate and share information." Despite the efforts of the Obama administration to integrate Web 2.0 into government operations, and although certain components of the Department of Homeland Security (DHS) such as the Federal Emergency Management Agency (FEMA) have their own Facebook page, DHS blocks social networking site usage by most DHS employees. Due to cybersecurity, site management, and employee usage concerns, most DHS headquarters computers, although able to access government web pages like the White House website, cannot access any of the social networking links (including GovLoop, which was designed by a former DHS employee for purposes of social networking among government employees) and lack this online community interaction. In their Net Assessment for the Department of Defense, Mark Drapeau and Linton Wells point out, "Security, accountability, privacy, and other concerns often drive national security institutions to limit the use of open tools such as social software, whether on the open web or behind government information system firewalls" (Drapeau & Wells, 2009, p. v.). Although there are risks and issues that can arise with the implementation of social networking sites, DHS, its state-operated fusion center partners, and local law

enforcement agencies will have to weigh the costs versus the potential benefits that could come with the integration of new technologies. As Drapeau and Wells state, "There is a point at which a mission can be hurt by strictly enforcing such draconian approaches that it keeps government from taking advantage of social tools that adversaries and other counterparties are using" (2009, p. 23).

According to a DHS official, state-operated fusion centers may also not be utilizing social networking sites in order to engage the public in the homeland security mission. The Department of Justice and Department of Homeland Security's "Fusion Center Guidelines" define a fusion center as "an effective and efficient mechanism to exchange information and intelligence, maximize resources, streamline operations, and improve the ability to fight crime and terrorism by analyzing data from a variety of sources" (United States Department of Justice [USDOJ] & United States Department of Homeland Security [USDHS], 2006, p. 2). Intelligence and information sharing via fusion centers is a key element to the overall homeland security mission; it is impossible for the federal government to have sole responsibility for homeland security and to accomplish nationwide effectiveness from the confines of Washington, D.C. Because fusion centers are regional entities, they have the capability to obtain information at a grassroots level, and they have the advantage of knowing state and local dynamics. If there are suspicious or potential terrorist activities occurring, it is likely that the fusion centers (and consequentially, local law enforcement officials) will know first. Judy Woodcock points out, "Citizens are, in fact, the very targets that terrorists seek. It is assumed that both the first preventers and first responders are likely to be civilians, but there is no system in place for Homeland Security Officials and responders to capitalize on the public's knowledge" (2009, p.2). The relationship between local law enforcement and local citizens can often yield valuable information that can lead to the discovery of dangerous activity. Therefore, the public's involvement in homeland security operations is a necessity.

The 9/11 Commission recommended that information sharing among various government entities at the federal, state, and local levels become a priority. The result has been that many states have adopted the fusion center approach (Riegle, 2009, p.2).

Today, there are over 70 fusion centers that are recognized by DHS. (Riegle, 2009). These fusion centers allow for information flow between state and local law enforcement officials, DHS, and other federal entities. Moreover, collaboration among all levels of government, including the private sector is imperative in order for counterterrorism initiatives to have any measure of success (USDOJ & USDHS, 2006, p. 14). Although fusion centers may be beneficial to homeland security efforts, gaining public trust in fusion center operations and encouraging citizens to participate in information sharing alongside fusion centers remains a challenge.

Two of the primary hurdles to the introduction and integration of social networking sites into the fusion center framework will be manpower and privacy issues. Because social networking sites such as Twitter and Facebook involve personal information about their users, individual citizens may be hesitant to allow state or local government entities to have access to their personal information. Manpower in fusion centers may also pose a problem: who will be in charge of monitoring and updating the social media sites in a timely manner? Social networking sites need to be maintained on a real-time basis in order to be effective; the public will likely lose interest and seek other avenues of information if a fusion center or police department's sites are lagging behind. Another issue is the verification of the accuracy of information that is relayed by citizens to fusion center or local law enforcement sites via social media.

B. RESEARCH QUESTION

How can state-operated fusion centers, in conjunction with local law enforcement agencies, utilize social networking technologies in order to strengthen their relationship with citizens within their communities and subsequently strengthen homeland security efforts? This query raises secondary questions:

- How has Web 2.0 evolved over the past year and been introduced/integrated within the operations of homeland security entities at the federal, state, and local levels?

- What are the implementation issues associated with the use of social networking technologies within fusion centers, as well as the homeland security and law enforcement frameworks? Specifically, what privacy, administrative law, and cybersecurity issues might homeland security and law enforcement entities encounter when attempting to integrate Web 2.0 and social media into their everyday operations?
- How can social networking technologies, in their current form, be utilized to bridge gaps between the public and fusion centers seeking to foster communication and collaboration between public citizens and the local law enforcement community?

C. ARGUMENTS

What is yet to be understood about the issue of integrating social networking sites within fusion center frameworks is the level of acceptance and usage of social networking sites by both the public and fusion center personnel in the counterterrorism/homeland security realm. Fusion center personnel and the public would have to accept and realize the value of using social media sites regularly in order for the concept to be effective. Although utilization of social media sites is currently free, fusion centers and local law enforcement agencies will need to integrate programs such as Twitter and Facebook into their daily operations, which will require resources to support the added staff responsibilities and the training of personnel who may be unfamiliar with social networking sites. Information technology (IT) support for regular troubleshooting issues, as well as address cyber-related issues in the event the servers or sites go down during an incident, will also be required.

However, utilization of Web 2.0 technologies, particularly social media, within fusion centers and local law enforcement entities is important because these networking sites could enable a more expedient exchange of information among fusion centers, law enforcement, and the public. The ability to collect and disseminate information on a real-time basis via fusion centers and law enforcement is a key element to the overall success of the homeland security mission; it is impossible for the federal government to have sole

responsibility for safeguarding the homeland from the confines of Washington, D.C. Because fusion centers are state and local entities, they have the capability to obtain information at a grassroots level, and they have the advantage of knowing the local environment and potential targets and vulnerabilities. If there are suspicious or potential terrorist activities occurring, it is likely that the fusion centers (and consequently, local law enforcement officials) will know prior to the federal government. Furthermore, the average citizen is more likely to notice abnormal activity in his city or community than an outsider; therefore, building a relationship between law enforcement and local citizens could lead to a valuable information exchange that would otherwise go untapped. In effect, social media, if leveraged appropriately, could enhance communication among fusion centers, law enforcement, and private citizens to better detect and deter terrorism.

Despite the advantages of integrating social media within the fusion center framework, there are many potential challenges. The adoption of Web 2.0 technologies, specifically social media, into fusion centers will not happen overnight. Technology is a rapidly changing phenomenon, and there must be procedures in place for fusion centers to govern the usage of social media sites in order to avoid abuse by personnel and to provide safeguards against various forms of nefarious activity. Hackers, viruses, the potential divulging of proprietary information, problems verifying authenticity and ensuring transparency of information, phishing, and the effect on employee productivity are among the many concerns that will need to be addressed by fusion center and law enforcement leadership along with IT personnel prior to social media implementation. All social media outlets that are adopted will need to be updated on a real-time basis to maintain viability, and there is currently no existing research in place on what constitutes an appropriate level of citizen involvement within the fusion centers and the homeland security framework. There is the risk that overzealous members of the community would communicate inaccurate or incomplete information to their fusion center or police department, and in the worst case, members of a community might communicate false information to their fusion center intentionally. Further complicating matters, the more than 70 fusion centers currently in existence are state-operated; therefore all are built independently and structured differently. Although there are fusion center guidelines in

place, they are only guidelines, not mandates, and fusion centers fashion themselves according to their individual needs. And although it is unlikely that social media technologies are widely used in fusion center operations today, they have the potential to improve communications between members of the homeland security community and the public.

Exploring the use of social networking sites in fusion centers is warranted because of the potential homeland security benefit that could result. According to statistics, Facebook has over 500 million active users (70% of whom are outside the United States), and people spend over 700 billion minutes per month interacting on Facebook's platform (http://www.facebook.com/press/info.php?statistics). As millions of Americans continue to join social media sites, DHS, fusion centers, and local law enforcement agencies can leverage that usage to increase awareness of potential nefarious activity and to strengthen communication between fusion center personnel and local citizens—that same local citizens who will likely be the first to become aware of potential terrorist activity.

The greater the level of communication among fusion center, law enforcement personnel, and local citizens the greater the chances of thwarting a terrorist plot or mitigating the damage of an attack. This research will explore the social networking avenues available to do that, including some that are working in practice, as well as the potential benefits and implementation challenges of integrating social media into the fusion center framework and the local law enforcement framework.

D. SIGNIFICANCE

At this point in time, there has been very little to no academic research conducted on social media integration into fusion centers, so the contribution of this thesis will be new. Greater attention is now being paid to federal, state, county, and city social media policies; a GoogleNews search yielded multiple web articles on social media integration into federal, state, and local governments on a daily basis. This thesis may be a platform and starting point for social media integration into various facets of the homeland security community via fusion centers and other local law enforcement entities. The immediate consumer of the thesis will be the fusion center community, law enforcement

officials, and DHS officials at a policy level. In order for homeland security efforts to be at their peak effectiveness, citizens must become an integral part of a collaborative homeland security community. Social media provides the platform for that collaboration to take place. Without it, homeland security efforts will lag behind, and vital information could potentially slip through the cracks, which, as was learned on September 11, could result in disastrous consequences. This research will explore some of the social networking avenues currently available to achieve the necessary level of collaboration among fusion centers, local law enforcement and the public.

THIS PAGE INTENTIONALLY LEFT BLANK

II. LITERATURE REVIEW

This literature review focuses on the myriad of issues surrounding the potential utilization of social media by state-operated fusion centers and local law enforcement agencies in order to strengthen their relationship with citizens in their communities and subsequently strengthen the homeland security mission. Specifically, this review examines existing literature on various aspects of social media and the ways in which these technologies could benefit or potentially hinder homeland security efforts in state-operated fusion centers in conjunction with local law enforcement entities. Because the integration of social media into the national security realm is multifaceted, several separate issues were examined.

Areas covered by this literature review include:

- Web 2.0 as it relates to social media and its ongoing integration into the national security paradigm;
- Privacy and other administrative law issues as they relate to social media;
- Fusion center guidelines and their potential evolution to include social media;
- Cybersecurity and its potential impact on social media integration into the homeland security paradigm.

A. WEB 2.0 AND SOCIAL MEDIA

- *How has Web 2.0 evolved over the past year and been introduced/integrated within the operations of homeland security entities at the federal, state, and local level?*

Recent publications regarding the involvement of the private sector and public citizens in the federal government seem to agree that in order for the federal government to be transparent and for homeland security efforts to be at their peak, members of the public need to feel that they are part of the homeland security mission and that they have the ability to communicate with their government. According to scholars such as Short

(2008), Bach & Kaufman (2009), Carafano (2009), and Bunt (2008), the number of people using Web 2.0 and social networking technologies will continue to grow and will inevitably impact the federal government. Web 2.0 is a key element to "breaking down barriers" between the government and its citizens (Short, 2008, p. 30).

According to Robert Bach and David Kaufman:

> Today's asymmetric threats have changed the way we think about the world and the compact between the federal government and the public. The initial round of homeland security strategies has not yet caught up with this global and internal transformation. While the nation fights overseas, a new social compact at home is needed that redefines opportunities and responsibilities just as much as world events are changing the risks and challenges to the American way of life. (2009, p. 11)

Bach and Kaufman assert that the new era of homeland security will rely largely on American citizens and their interactions with the government:

> Effectiveness [of homeland security initiatives] will fall as much (if not more) on the capacities of local communities, neighbors, and families, than on federal response teams and billions of dollars of new equipment. The challenge is to understand how to engage the public *collectively and on a large scale* across the nation to build this capacity. (Bach & Kaufman, 2009 p. 3)

Although the federal government is making efforts to integrate social media within its agencies, scholars such as James Carafano believe that they still have a long way to go. As more and more agencies continue to adopt Web 2.0 applications and social media into their agencies, the technology will expand into the realm of homeland security. The government needs to take the necessary steps to get in line with the emerging technologies (Carafano, 2009, p. 1). There are several obstacles that agencies may face, however, when attempting to adopt any new technology. These include lack of access, security and privacy concerns, resource and budgetary issues, as well as legal restrictions and terms of service restrictions. Carafano suggests that Congress direct the National Academies to conduct a study on national security and social networking (2009, pp. 4–5); however, he does not discuss how conducting such studies could slow the rate

of federal adoption of social networking technologies. By and large it appears as though many federal entities have forged ahead to adopt independent social media policies.

Additional concerns arise with government adoption of social media due to the existence of hackers, viruses, the potential risk of divulging of proprietary information, the problems of verifying authenticity and ensuring transparency of information, phishing, and concerns regarding employee productivity. Institutions, including the Federal government, must take precautionary steps when considering the incorporation of Web 2.0 into their daily business practices (Short, 2008, pp. 29–31). Researchers propose adopting policies to govern social media site usage and instituting controls to help ensure successful integration (Bunt, 2008, pp. 42–43). Even if successful, the integration of social media will be engender cultural implications across all agencies who attempt to adopt Web 2.0 technologies; there will be a change in the dynamics of the way agency offices communicate with one another and with the private sector. (Godwin et al., 2008, pp. 1–2). Federal, state, and local government agencies will need time to explore their budgets in order to allocate the appropriate resources.

Although the use of social media in the federal government has been largely inconsistent, it has increased exponentially over time. Some agencies, such as the Department of Defense (DoD), and the Department of State have recently allowed the use of social media within their agencies (McCullagh, 2010, n.p.). In 2009, the Central Intelligence Agency (CIA) invested in Visible Technologies (who is partnered with Q-Tel). “The investment in Visible is part of the CIA’s effort to harness ‘open source intelligence’—intelligence that’s publically available through television or the Web, but that is easily buried by each day’s deluge of information” (Sullivan, 2009, n.p.). This increase in social media adoption throughout the federal government is indicative of a shift in the way that the government interacts with other agencies and with the American public.

Although the idea of using social media is catching on within federal, state, and local governments, the idea of incorporating social media into state-funded fusion centers is a concept that has gone relatively unexplored in academia. There are recent master’s theses written by former Naval Postgraduate students pertaining to some aspects of Web

2.0 and its integration into the national security paradigm. These theses represent the most current studies conducted in the areas of Web 2.0/social media/intelligence communities and their relation to homeland security.

According to Adrienne Werner, the key to successful implementation of Web 2.0 will involve leadership adaptation, as well as training of personnel and outreach to the homeland security community (2008, p. 39). Research indicates that in order for social media to successfully integrate within an agency, government personnel who are responsible for using the technology must be motivated to use it. Best practices for the implementation of new media include encouraging participation, a shift from a "need to know" mentality previously prevalent in many national security agencies to a "responsibility to provide" mentality, managing the user community, implementing standards of conduct, and encouraging collaboration (Werner, 2008, p. 55). As Werner illustrates, the introduction of new technologies may produce some resistance by new users. Not all fusion center personnel (or their leadership for that matter) will be familiar with social media, and there will have to be an obvious value added in order for fusion center leaders to buy in to the concept and move forward with developing social media policies.

Research suggests that the benefits of using social media technologies will outweigh the initial implementation challenges. For example, the growing use of social networking sites by state emergency responders illustrates the importance of citizen involvement in emergency situations (Van Leuven, 2009, p. 15). Following the 2007 southern California wildfires, Van Leuven performed a case study involving social media usage in San Diego that enabled cross-communication between first responders and citizens. She found that "[a]ccurate and expedient information sharing with the public is critical to citizens and local jurisdictions during emergency response and recovery. As such, strategies that leverage all resources and information interactively results in stronger communities that are more resilient and can bounce back quicker from a disaster" (2009, p. 89). Use of Twitter during emergencies not only gives emergency

responders and citizens immediate access to real-time information and maximizes responder and citizen communication, but it also conserves resources (Van Leuven, 2009, p. 35). That kind of instantaneous communication can ease public tensions; in fact, citizens appear to rely on social networking sites as one of their primary sources for information and have even crashed these websites during emergency situations (Van Leuven, 2009, p. 57). Some emergency responders who had qualms about utilizing social networking technologies noted a lack of resources, distrust of tools and content, use of unfamiliar technology, lack of support from leadership, and information overload as the primary reasons for not using social media when responding to emergencies (Van Leuven, 2009, pp. 76–78).

Despite any doubts that first responders or other government officials may have about the use of social media, the fact remains that public citizens will most likely be the first people to know about a terrorist attack, natural disaster, or other catastrophic incident in their community. Engaging them in homeland security efforts via social networking is imperative in order to "capitalize on the public's knowledge" and strengthen the overall homeland security mission (Woodcock, 2009, pp. 2–3). And although there could be an initial strain on resources at the onset of social media integration, once personnel are trained and adapt to social media use as part of their daily operations, resources may actually be saved. "With the development of social media, we now have the best possible opportunity to engage the public with little or no impact on fragile government budgets" (Woodcock, 2009, p.1). Once social media is integrated, however, the next question will be *whom* the government entities should be listening to. Woodcock proposes "a model in which social media is applied to an existing trusted network in the community. Most jurisdictions have a group or groups of trusted agents such as amateur radio operators, search and rescue volunteers, citizen corps representatives or neighborhood response networks" (Woodcock, 2009, p. 59).

Overall, the recent theses reflect a growing awareness of social media and the need to incorporate new technologies into the national security platform. The drawbacks they note are similar: resistance to new technology by personnel, allocation of resources, misinformation or an overabundance of information ("rumor control" issues), and the

overzealous citizen participant. Again, what is lacking in current research is how social networking and citizen participation could potentially benefit fusion centers.

Along with a variety of publications, social media has garnered much attention by federal professionals in the form of roundtable discussions, forums, conferences, and workshops. There have been recent efforts by the General Services Administration (GSA) to encourage the use of social media within federal agencies by way of conferences. The Social Media for Communicators Conference in March of 2008 illustrated the benefits to agencies of social media such as blogging to get information out to the public (Godwin, 2008, slide 11). The theme of the conference was apparent: the federal government needs to utilize Web 2.0 technologies.

For example, an "Expert Round Table on Social Media and Risk Communication During Times of Crisis" met on March 31, 2009, at the American Public Health Association headquarters in Washington, D.C. The panel found that, by and large, emergency managers and entities such as the American Red Cross and the Centers for Disease Control are capitalizing on social media to push messages out to the public in disaster situations. "Especially in times of emergency, social media can and should be employed to transmit critically important information immediately to as many people as possible" (Currie, Tinker, & Fouse, n.d., p.2). The report also discussed the role that social media played in getting information to the public during the Virginia Tech shootings, the terrorist attack on Mumbai, and the national peanut recall due to salmonella (Currie, Tinker, & Fouse, n.d., p.1). The roundtable panel also found that members of the public who use social media to liaise with first responders partake because they *want* to opt-in to the discussion (Currie, Tinker, & Fouse, n.d., p. 5). To continue those kinds of conversations, governments may need to change the tone of their communications with the public. "To engage communities in new ways, advocate rather than preach. Instead of thinking of 'transmitting' messages, especially during an emergency, allow people to engage and participate. When possible, the style should be informal and conversational and should work to inform and collaborate with an audience—not command and control it. Above all … build a community" (Currie, Tinker, & Fouse, n.d., p.10).

In 2009, the Department of Homeland Security hosted the "The Ogma Workshop: Exploring the Policy and Strategy Implications of Web 2.0 on the Practice of Homeland Security." The workshop was designed to share best practices and discuss the way forward for integrating Web 2.0 into federal emergency operations and public safety arenas (Kubota, 2009).

Tim O'Reilly's Gov 2.0 summit was held in Washington, D.C. on September 7–8, 2010. The conference examined the future of Gov 2.0 technologies and their potential impact on the government and the private sector. "Our goal at the Gov 2.0 Summit is to bring together innovators from government and the private sector to highlight technology and ideas that can be applied to the nation's great challenges" (O'Reilly, 2010).

Although there are many risks associated with the federal government's adoption of Web 2.0., Drapeau and Wells assert that, by remaining stagnant and refusing to integrate Web 2.0, agencies could potentially cause more long-term harm than good (2009, p. 23). The general consensus across the current spectrum of research is that Web 2.0 and social media are here to stay and will continue to be rapidly adopted by the government, businesses, and citizens. Researchers agree that federal, state, and local governments (and ultimately homeland security) will inevitably be affected by social media and should take immediate steps to integrate these technologies into everyday agency operations. What is left to be explored is how fusion centers should be leveraging these technologies.

B. PRIVACY AND OTHER ADMINISTRATIVE LAW ISSUES

- *What are the implementation issues associated with the use of social networking technologies within fusion centers as well as within the homeland security and law enforcement frameworks? Specifically, what privacy, administrative law, and cybersecurity issues might homeland security and law enforcement entities encounter when attempting to integrate Web 2.0 and social media into their everyday operations?*

A major concern with federal or state involvement in social networking is the issue of privacy. Personal privacy is an ambiguous concept that is not easily defined

(Solove, 2008). In order for a social networking policy to work across the federal government and DHS (and potentially have a positive trickle-down effect to state and local fusion centers), strong privacy protections will need to be crafted and implemented in addition to those that already exist. A workshop entitled "Government 2.0: Privacy and Best Practices" took place in June of 2009 and focused on the privacy hurdles in adopting Web 2.0 into federal agencies. Much of the social media currently in place requires a user sign-up that tracks a user's personally identifiable information. Members of the workshop panel seemed to agree that privacy issues will play a major part in the integration of social media into federal agencies.

Because privacy is a loosely defined concept, identifying what exactly jeopardizes privacy and formulating solutions to safeguard privacy is a difficult venture (Solove, 2008, p. 2). How can a society foster and appreciate its privacy and enforce privacy laws when few seem to know what "privacy" issues really are? Furthermore, if society is unable to define privacy, how can laws be enacted in order to protect it? Because a holistic definition of privacy does not exist, it is difficult for the federal government and the American public to decide how privacy pertains to them and to what degree they wish to guard their privacy. Simply put, "people have a hard time articulating privacy preferences," (Sadeh et al., 2007, p. 411). Researchers suggest starting with a conservative approach when dealing with privacy matters and relaxing the guidelines over time. Doctrine does not exist on a federal level insofar as adopting Web 2.0 and social networking policies that allow fusion centers to liaise with the public, nor do guidelines exist on the privacy protections that would need to be implemented at the onset of social-network site integration into fusion centers, although some of these policies may exist on an individual state-operated fusion center basis. The federal government might also encounter problems when reviewing the privacy policies of social networking sites. As noted during the privacy workshop, the federal government is "playing in [social media's] field" when it comes to the privacy policies of social networking sites.

Because fusion centers examine the activities of the American public, federal and state privacy laws are evoked that have to be addressed. Fusion center guidelines

published by DHS and the Department of Justice (DOJ) provide a roadmap for the implementation of state-operated fusion centers as well as an explanation of privacy laws that must be adhered to in order to safeguard PII and maintain public trust. The "Civil Liberties Impact Assessment for the State, Local, and Regional Fusion Center (SLRFC) Initiative" also provides avenues of redress in instances where a member of the public feels that his or her rights have been violated (USDHS, 2008a, p. 4). However, none of the fusion center guidelines or assessments currently addresses the issue of incorporating social networking sites into fusion center frameworks.

In 2008, DHS performed a "Privacy Impact Assessment for the Department of Homeland Security State, Local, and Regional Fusion Center Initiative." The document stresses the importance of adhering to privacy laws and conducting regular privacy training for fusion center personnel. DHS seems to recognize that privacy issues are not stagnant and will need to be reevaluated over time. "As the SLRFC Initiative evolves in the upcoming months and years, this Office will continue to revisit [privacy] issues of concern and evaluate new issues that may arise. As Congress, the President, and [DHS] have recognized, fusion centers are key to sharing information that may prevent threats to our Nation. At the same time, we must ensure information is shared in accordance with the law" (USDHS, 2008b, p.6).

As a follow-up, in June of 2010, DHS and DOJ published "Privacy, Civil Rights, and Civil Liberties Compliance Verification for the Intelligence Enterprise." Intended for fusion centers, the document contains various questionnaires to measure fusion center compliance with privacy standards and other administrative procedural laws. "Compliance reviews and audits have become a necessary tool for agencies to use in order to identify high-risk operational and management issues, particularly with the recent development of fusion centers.… This compliance verification will assist intelligence enterprises with ensuring their compliance with all applicable privacy, civil rights, and civil liberties protection laws, and policies while sharing intelligence information needed to safeguard America" (USDOJ, 2010, p. 2).

Recently, DHS privacy policies as they pertain to social media were put to the test. The National Operations Center (NOC) in the Office of Operations Coordination and

Planning (OPS) reviewed information posted on social media sites to aid in disaster relief efforts after the earthquake in Haiti, which required a privacy impact assessment (PIA). Called the Haiti Social Media Disaster Monitoring Initiative, the NOC worked in "identifying, using, disseminating, and maintaining this information to comply with its statutory mandate to provide situational awareness and a common operating picture for the entire federal Government, and for state, local, and tribal governments as appropriate, and to ensure that critical disaster-related information reaches government decision-makers" (USDHS, 2010, p. 3).

The initiative also illustrated one way that a federal operation can utilize social media, effectively filtering large amounts of information and verifying it for accuracy. "The NOC identifies information from third party hosts submitted voluntarily by members of the public and compares that information with information available in open source reporting and through a variety of public and Government sources. By bringing together and comparing many different sources of information, the NOC will attempt to generate a more accurate picture of activities occurring in Haiti" (USDHS, 2010, p. 3). There is no guarantee, however that all information obtained will be 100% accurate. "Users may accidentally or purposefully generate inaccurate or erroneous information. There is no mechanism for correcting this. However, the community is largely self-governing and erroneous information is normally expunged or debated rather quickly by others within the community with more accurate and/or truthful information" (USDHS, 2010, p. 9).

The report also addresses the critical privacy issue of collecting personally identifiable information (PII) from the public. According to the report, during the Haiti initiative, PII "is not collected, retrieved, shared or retained. Information is only collected to provide situational awareness and to establish a common operating picture" (USDHS, 2010, p. 7) Additionally, it is noted that all DHS staff are required to undergo privacy training (USDHS, 2010, p.10).

Although the NOC only monitored social media sites and did not engage in a two-way dialogue with the public in which they received information directly from individual

social media users, the Haiti exercise illustrates that social media can, in fact, be used as an effective means to retrieve viable and accurate information from the public (USDHS, 2010, p. 2).

The NOC's Haiti initiative reflects both DHS awareness of privacy laws as well as its due diligence to follow them. Members of the public monitor privacy law compliance to ensure that those laws are being followed. There are watchdog groups in existence, such as the Electronic Privacy Information Center (EPIC) based in Washington, D.C., that has published reports on FOIA requests that their center has filed regarding the data collection process of various fusion centers and gives "latest news" updates on fusion center privacy-impact analyses while tracking Congressional actions on laws impacting privacy matters (Electronic Privacy Information Center [EPIC], 2010).

Despite apparent efforts of agencies such as DHS to adhere to privacy laws, 1500 AM, Federal News Radio reports that, although social media are helping to foster communications between the government and the public, there remain several administrative law implications that have not been completely addressed—such as record keeping requirements, privacy issues, FOIA, and the Paperwork Reduction Act. "After analyzing federal policies and reports, and interviewing officials at selected federal agencies such as the Department of Homeland Security and the General Services Administration, the GAO found that these technologies can actually increase the risk of improper management and exposure of government records and sensitive information" (Wilshusen, 2010a).

To begin to address these administrative law and process issues, in July 2010, Gregory C. Wilshusen, director of Information Security Issues for the Government Accountability Office (GAO) testified before Congress on the challenges facing federal agencies as they move forward to adopt Web 2.0 technologies. Wilshusen testified that, as of July 2010, "22 of 24 major Federal agencies had a presence on Facebook, Twitter, and YouTube" (Wilshusen, 2010b, p. 3). Wilshusen discussed the growing use of social media and the implications that usage has on privacy laws, FOIA, and record keeping requirements for agencies. As agencies move forward with social media and other Web 2.0 technologies to create bridges of communication with the public thereby "allowing

citizens to become more involved in the governing process and thus promoting transparency and collaboration, … determining the appropriate use of these new technologies presents new potential challenges to the ability of agencies to protect the privacy and security of sensitive information, including personal information, shared by individuals interacting with the government and to the ability of agencies to manage, preserve, and make available official government records" (Wilshusen, 2010b, p. 13).

What is lacking in current research is how privacy is impacted in practice: i.e., when fusion centers integrate social networking sites into their daily operations to liaise with the public. There is a gap in research in the privacy portions of fusion center guidelines regarding social networking sites (for more on fusion center guidelines, see the following section).

C. FUSION CENTERS

The more than 70 fusion centers currently in existence across the United States allow for information flow between state and local law enforcement officials, DHS, and other federal entities. Current guidelines note the dire need for collaboration across federal, state, and local governments. Moreover, collaboration between all levels of government and including the private sector is imperative in order for counterterrorism initiatives to have any measure of success (USDOJ & USDHS, 2006, p. 14). More specifically, fusion center guideline 18—"develop and implement a communications plan within the fusion center; among all involved law enforcement, public safety, and private sector agencies and entities; and with the general public"—stresses the importance of cross-communications via electronic and other media (USDOJ & USDHS, 2006, p.65). Although social media is not specified in the current guidelines, it is reasonable to assert that, with the growing amount of attention being paid to Web 2.0 across the federal government, social media may be an item addressed in future fusion center guidelines.

A report published by the International Association of Chiefs of Police (IACP), Homeland Security Committee, discusses the way ahead for fusion centers. The report states that fusion centers need to, "[h]arness and apply the collective knowledge of their constituents to address issues related to threat and risk," (IACP, 2010, p.1). Clearly the

fusion center enterprise is no longer a one-way intelligence venture. Now, the fusion center mandate has grown to include state and local law enforcement partners as well as the public. “Fusion centers are finding increased relevance among their state and local consumers, and the benefits of information and intelligence sharing are begging to be realized” (IACP, 2010, p.2).

The IACP implores fusion centers to develop future strategic plans that will foster cross communications and “revisit their business models to ensure that they are aligned in a manner that will embrace collaboration and information sharing to meet the demands of both present and future. Then begin connecting and establishing relationships with diverse partners to share information needed to tackle the problems inherent to crime and homeland security” (IACP, 2010, p.6). Among IACP recommendations is that fusion centers “promote and advance Web 2.0 and other enterprise technologies that support collaboration and knowledge production” (IACP, 2010, p.6).

Because there currently exists no overarching “how-to” guidance or published best practices regarding implementation of social media technologies into fusion centers, the adoption of social media policies could be considered to be largely at the discretion of the individual fusion centers themselves. There is presently no research on allocation of resources when implementing social media technologies, nor is any federal literature available for fusion center personnel on the appropriate use of social media to interact with the public.

D. CYBERSECURITY

From the perspective of integrating social media into fusion centers and local law enforcement agencies, cybersecurity will play an integral part in ensuring that communication between fusion centers and citizens does not result in compromising vital homeland security information or the private information of members of the public. Cybersecurity is a very broad topic, and although research on how to strengthen the nation’s cybersecurity infrastructure started years ago, recently, there has been a greater attention paid to cybersecurity by both Congress and DHS. The Congressional Research Service (CRS) has published a number of comprehensive reviews of potential forms of

cybercrime or cyberterrorism and policy considerations for Congress. The 2007 CRS Report worked to define cyber-related terms and potential objectives of cyberterrorists or criminals. There are varied perceptions regarding what constitutes an actual cyberattack, and not everyone considers cyberthreats to be a major vulnerability (Rollins & Wilson, 2007, p. 5). In the past few years, cyber threats have moved to the forefront of homeland security initiatives. There is concern that the progression of cyberattacks over time will move from the disruption of networks and other critical cyberinfrastructure to their complete destruction (Rollins & Henning, March, 2009, p. 3). It also remains unclear where the origination of a cyberattack could occur; attacks may not necessarily stem from terrorist organizations and may come from foreign enemies. Therefore, forthcoming policy must center around the "enhanced sharing of timely and relevant cyber security related plans and risk data," (Rollins & Henning, March, 2009, pp. 4-6). Another element explored by the CRS is the issue of legal authorities and policy considerations regarding cybersecurity in the United States. Forthcoming legal issues will arise when assigning responsibility and authority for cybersecurity enforcement across the federal government. Legislation may need to change to ensure that measures taken fall within privacy laws and comply with the Constitution (Rollins & Wilson, 2007; Rollins & Henning, 2009). All of the current CRS reports explore the issue of cybersecurity and the legal authorities (and complications) that surround protecting critical cyberinfrastructure, which will invariably impact the cybersecurity precautions taken by the federal government. This could pertain to fusion centers as far as assigning responsibility for cybersecurity enforcement within the fusion center framework, be it fusion center personnel, DHS, or the social media sites.

Beyond cyberattacks, another cyber-related concern regarding social networking site usage by the federal government is social engineering by hackers. Research conducted on the impacts that hackers can have on homeland security networks and private sector businesses places a great deal of emphasis on training and retraining personnel involved with sensitive information (Granger, 2002, p. 3). Because hackers would be unlikely to have an in-person encounter with a homeland security professional or a member of the public who networks with their fusion center, the odds are that the

attack would come via impersonation; hackers would have the potential to obtain the personal information of citizens liaising with their fusion centers by impersonating homeland security professionals on social networking sites. Although not as harmful as some other forms of internet attacks, hackers have the potential to disrupt the integrity of the sites and the relationships that state and local law enforcement may form with the public. There is no current literature available on how fusion center personnel could be trained to avoid this type of nefarious activity when communicating with the public.

A recent symposium on cyberdeterrence initiated by the Homeland Security Policy Institute (HSPI) shed light on potential forthcoming doctrine and initiatives taken by both the United States and the international community to secure cyberinfrastructure. Several general themes emerged. The panelists agreed that the advantage of cyberthreats lies with the attacker and that attacks are a asymmetric vulnerability. The potential vulnerabilities for cyberattacks are critical infrastructure, the disruption of data, and foreign attacks (HSPI, 2009, session 1). The United States faces limitations in thwarting attacks because it is difficult to threaten unknown entities. The general perception is that cyberterrorism doesn't really exist as a threat currently, but preparedness and resiliency of networks and cyberinfrastructure are key to deterrence. Over time, definitions of what actually constitutes a cyberattack will solidify and attribution will become a cornerstone of deterrence and cyber-protection policy (HSPI, 2009, session 2). Panelists also recognized that there are daily attempts to hack into homeland security networks and private sector websites. Part of the issue with thwarting attempted attacks is the reluctance of Internet service providers to get involved in Internet policing as they view themselves only as an international platform for the Internet. A common international lexicon regarding cyberdeterrence would be of great benefit when looking to strengthen cybersecurity and cybernetworks globally. Initiatives may be taken by the administration to institute incentives for private-sector organizations and citizens to regulate themselves as opposed to instituting regulations. Imposing minimum cyber-protection standards throughout the government and the private sector could help strengthen the cybernetworks across the United States (HSPI, 2009, session 3). Panelists agreed that the 60-day cyber policy review instituted by the Obama administration will help increase

public awareness of cyberthreats. Collaboration, not solely information sharing, is the key to the future success of cybersecurity (HSPI, 2009, session 4). Although the symposium did not delve into fusion centers, law enforcement, and their use of social media per se, the topics discussed were indicative of the direction in which U.S. cyberdeterrence policy is headed, impacting the way that homeland security networks are operated in the future. These issues will likely become doctrine over the course of the next year and will grow in relevance during the incorporation of Web 2.0 into the federal government and fusion centers.

Also in 2009, the CIO Council published "Guidelines for Secure Use of Social Media by Federal Departments and Agencies." The guidelines state that, "the use of social media and the subsequent cyber security concerns form a complex topic that involves, not only familiar threats, but also introduces additional vulnerabilities, targeted by an advanced threat, requiring updated sets of controls" (CIO Council, 2009, p. 8). The guidelines also seek to warn agencies that adequate protections must be put in place in order to safeguard social media sites and to protect cyber infrastructure. "As the Federal Government begins to utilize public social media websites, these advanced persistent threats may target their efforts against these websites. These attackers may use social media to collect information and launch attacks against federal information systems" (CIO Council, 2009, p. 9).

There is an overall consensus of professionals in the field of cybersecurity that cyberthreats will become more prevalent as time goes on. A 2010 web-based news report in "Government Technology" states that, "[a]lmost all experts agree that the private and public sector aren't coordinated enough to avoid nightmare cyber-security scenarios, and many have predicted a rapid increase in international tensions if such risks go unanswered, according to an EastWest Institute press release. They urged greater cooperation at the private, public and international levels" (Cyber-Security survey, 2010). Generally speaking, homeland security professionals cannot predict if and when a cyberattack will occur or what form it will take. There are significant gaps in research, mainly because many of the issues involving cybersecurity are only recently beginning to be explored. Because of the attention that cybersecurity is now receiving, there will likely

be a flood of research conducted in the upcoming year, which may eventually lead to the use of social media by fusion centers/local law enforcement as it continues to evolve.

E. CONCLUSION

- *How can social networking technologies, in their current form, be utilized to bridge gaps between the public and fusion centers seeking to foster communication and collaboration between public citizens and the local law enforcement community?*

There are currently several documents that have been published to serve as guidelines for establishing social media policies for federal agencies as well as state and local governments; these policies are now being generated on a regular basis. These documents generally examine employee usage of social media during work hours, who should be responsible for posting to and maintaining social media sites, and what messages are appropriate. The documents also address cybersecurity and legal and administrative issues, and they provide guidelines on how to structure a social media policy to engage with the public. For example, the state of Oregon's Department of Administrative Service ([ODAS], 2010) published guidelines for their state-operated agencies, describing the types of social media that are available and sample social media sites that are already in use. In addition, for cities contemplating delving into the social media realm, the Penn Fels Institute of Government published a "lessons learned" manual of best practices gleaned from cities that have already successfully adopted social media policies (Kingsley, 2010). On the federal side, the Center for Technology in Government published "Designing Social Media for Government: Eight Essential Elements" (Hrdinova, Helbig, & Peters, 2010). The report describes a study conducted of 26 government documents on social media and 32 interviews with government staffers who were already using or working to develop social media policies (Hrdinova, Helbig, & Peters, 2010, p. 3). "While our sample of government policies is too small to draw any definite conclusions, local government policies tend to be more explicit on account management as compared to state or federal agencies" (Hrdinova, Helbig, & Peters, 2010, p. 6).

While federal, state, and local policy documents pertaining to social media surface on a daily basis and there has been an overall increase in workshops, forums, conferences, and symposia regarding social media, privacy, and cybersecurity, incorporating social media into state-operated fusion center frameworks to liaise with the public has been unexplored by academia to date. Current literature broadly addresses Web 2.0 and social media, privacy and other administrative law issues, fusion centers, and cybersecurity, but there are significant gaps remaining in the literature. Bodies of knowledge needing further exploration include doctrine on social media and its ongoing integration into the national security paradigm and how social media technologies can be used by fusion centers in conjunction with local law enforcement entities to increase collaboration with the American public. There will also need to be ongoing research in the areas of privacy and administrative law issues as well as cybersecurity as they relate to social media integration, as these issues will certainly evolve over time.

III. METHODOLOGY

A. METHODOLOGY

The research component of this thesis is qualitative. The researcher utilized the case study method to allow for in-depth analysis and discussion of practical viewpoints with interviewees that could not be gleaned by using a broad-ranging, one-dimensional questionnaire with numerous participants. The purpose of these three case studies was to determine what types of social media policies have been adopted by the individual entities and, based on their experiences, assess the potential benefits and challenges of adopting these technologies into the fusion center and law enforcement framework. The case studies were to act as a gauge to how integrating social media into the daily operations of a state-operated fusion center could aid in collaboration with local citizens to strengthen government/community relationships and thereby aid in strengthening the homeland security mission.

B. SAMPLE

In order to assess how social media could potentially benefit state-operated fusion centers, three case studies were conducted. These case studies were performed at the local law enforcement, fusion center, and public-safety department level. The case study participants, Deputy Chief Mark Stigler from the Waukesha, Wisconsin, police department; Aaron Kustermann, Chief Intelligence Officer for the Illinois State Police, who oversees all intelligence collection and response operations for the Illinois fusion center, known as the Statewide Terrorism and Intelligence Center (STIC) as well as field intelligence personnel; and Colonel Keith Squires, Deputy Commissioner for the Utah Department of Public Safety in Salt Lake City, Utah, were solicited by utilizing current DHS and Center for Homeland Defense and Security contacts. These entities were selected by the researcher because they facilitate social media practices in three separate states, and all have various homeland security responsibilities at the local and state level. Because the entities operate in different areas of the country, they have different

constituency bases, operating procedures, and leadership, which the researcher leveraged in order to gain insight as to how social media implementation could potentially affect state and local government entities on a broader spectrum nationwide. All three interviewees had the autonomy to make decisions about the implementation of social media technologies in their agencies and had the most insight as to their current and potential effectiveness.

C. DATA COLLECTION

Data was collected by compiling a set of interview and secondary questions to ask the participants to identify and discuss the kinds of Web 2.0 technologies, specifically social media, that their individual agencies are currently utilizing, and how their use has affected their positions, relationships with other homeland security partners, and relationships within their local communities. The interviews were also structured to glean the participants' perceived outlook for future social media technologies as it applies to their current position. Participants were sent the interview questions electronically and then telephone or Skype interviews were conducted, recorded, and transcribed by the interviewer. The transcribed notes were forwarded to the interviewees prior to publication to ensure integrity of content and accuracy of the interviewees' viewpoints and opinions, and to avoid divulging any confidential information that was relayed to the researcher during the interview process.

D. DATA ANALYSIS

Data was analyzed based on the respondents' current social-media usage, as well as their "perception of future usefulness" of social media within their law enforcement, fusion center, or public safety entity, as well as any anecdotal occurrences relayed by the respondents that portray the benefits or challenges of adopting social media. Generally, all interview responses were incorporated into the published portion of the case studies. The breadth of data analysis was dependent on the range of respondent's responses; the researcher looked to identify trends and common themes throughout the case studies in order to establish how these agencies utilize social networking technologies in order to

foster relationships with citizens (or other homeland security partners) within their communities and subsequently strengthen homeland security efforts. The data acquired from the case studies was also analyzed to identify how Web 2.0 technologies have impacted these various agencies and departments, including challenges they encountered while integrating new technology into their everyday operations. Because all three case studies produced data that alluded to a way forward for the use of social media in some capacity, the data analysis could serve as a potential baseline for agencies and departments looking to utilize social media and other various Web 2.0 technologies in the future.

The second step of this research project was to incorporate external sources (academic and media) to address the overarching push for social media incorporation into federal, state, and local government entities across the country. In order to gauge the potential impact that social media could have on fusion center and law enforcement framework, the external sources were broken down into several categories in an effort to identify specific areas that need to be examined when discussing the rise of Web 2.0 and social media and its various implementation issues. The following questions were considered:

- How has Web 2.0 evolved over the past year and been introduced/integrated within the operations of homeland security entities at the federal, state, and local level?
- What are the implementation issues associated with the use of social networking technologies within fusion center as well as the homeland security and law enforcement frameworks? Specifically, what privacy, administrative law, and cybersecurity issues might homeland security and law enforcement entities encounter when attempting to integrate Web 2.0 and social media into their everyday operations?
- How can social networking technologies, in their current form, be utilized to bridge gaps between the public and fusion centers seeking to foster communication and collaboration between public citizens and the local law enforcement community?

The goal of conducting a thorough literature review of these topics was to depict the ever-changing social media environment and its multiple implementation implications and to identify trends that affect social media adoption within various federal, state, and local government entities.

IV. CASE STUDIES

Research for this thesis involved three separate case studies: local law enforcement, a state-operated fusion center, and a public safety department. Each was at a different stage in the examination or use of social media within its particular entity.

A. CASE STUDY: LAW ENFORCEMENT

The first case study involved Deputy Chief Mark Stigler from the Waukesha, Wisconsin, police department. Although originally opposed to the use of social media for law enforcement and community liaison purposes, Stigler found himself at the helm of social-media integration for his department.

> Over the last year my city and my police department have explored the use of social media by employees. The progression has been tremendous due to a change in administration and a rapid change in attitudes. At first, due to fear of the unknown and fear of viruses, both the city and the department rejected the use of social media by employees. As time, personnel, and social attitudes changed, the idea of building a closely monitored policy to support employee use was considered to support the mission of municipal government and the police department. I find myself educating leadership as we go along. We have to show them how social media will work for them. (M. Stigler, personal communication, July 30, 2010)

Because every agency or department differs in mission and scope, the objectives of utilizing social media may differ. Stigler views social-media integration into his department as a way to reach out to the citizens of Waukesha to create an opportunity for them to communicate with their local law enforcement. The end result of that could equal a greater sense of wellbeing within the citizenry and result in a safer community.

> We have the opportunity to enhance communications with and enhance the safety of citizens by using Web 2.0 technologies. These technologies allow two-way interoperability and more importantly, collaboration across time and distance, in many areas critical to public safety and the effective operation of city government. This in turn builds community cohesion in times of serenity or strife. The next generation of emergency dispatching (NG911) will encompass all of these technologies including live streaming

> video as the new standards in communications. Our use of these modalities of communication now will allow for a smoother transition into the future of how we connect with our citizens. When I sell this concept to other agencies and disciplines I say, whether we want to use it is irrelevant. It's coming … it's here. The future of public safety is going to be built on the digital platform; we don't have any choice anymore. (M. Stigler, personal communication, July 30, 2010)s

The advent of social media may be inevitable; however, the drawbacks of social-media integration can present many challenges for entities attempting to weave instantaneous and real-time communications together with the public. For Stigler, the issue is resources:

> The biggest drawback is people to run the system. Many agencies do not have personnel with the training and desire to constantly post and read. Once the public gets used to or begins to rely on the system for info, you can't just post when you feel like it, you must IM, tweet or post quickly and accurately or the public will tune out or sue you for not keeping the site current during times of crisis. Another issue is the level of control and permissions to allow certain personnel to edit, add, and update the sites, blogs or IM's. You can't just let anyone edit as they may not have the maturity, knowledge or insight to speak for the city or the department. (M. Stigler, personal communication, July 30, 2010)

In addition to needing trained and available personnel, Stigler also recognizes that leadership has concerns that social media will open doors to the local government in a virtual sense, thereby adding to the vulnerabilities of their cyber infrastructure. "The biggest implementation issue has been the fear of viruses infecting the larger citywide computer system" (M. Stigler, personal communication, July 30, 2010).

Stigler also sees administrative issues as a hindrance to adopting social-media policies. For example, state laws on record keeping requirements for communications with the public have been receiving much attention on a national level. "If you allow anyone from the public to post on a site (good, bad or nasty); is the post part of a public record that must be maintained for seven years? Government records can't just be deleted or destroyed at will. Each agency must follow an approved records destruction plan that must be approved by the State" (M. Stigler, personal communication, July 30, 2010).

Although administrative issues loom, in Stigler's opinion social media can be used for more than counterterrorism efforts. In his view, social media gives his department the opportunity to post on issues that affect the community in real time, ultimately saving the city money and resources. Some of the issues he cited include: informing the public of downed power lines, meetings or public hearings, upcoming community events, water main breaks, pothole locations, tracking gangs or other criminal activity, protecting critical infrastructure, debating community issues, reporting storm damage, instant reporting during emergencies, daily messaging to keep the public and partners informed, tweeting press releases when posted, issuing updates on videos and photos, tweeting declarative statements regarding specific events and agency status, and road closures due to accidents or construction (M. Stigler, personal communication, July 30, 2010).

Even more important than keeping the public informed, in Stigler's view, is the potential impact that social media could have on those rare cases where lives are at stake.

> [Recently] we had a child enticement case that the police department handled in the old fashioned way. They came, talked to the victim and mother, took a report and put out an extra check on the roll call board. It soon disappeared from the police radar screen as more important cases came up. However, the citizens of the neighborhood did not let it drop. They banned together without the police and created on-line social media networks and spread the description of the suspect and his vehicle far and wide. Before we knew it, citizens were calling the police department wondering why we weren't involved in this system. Citizens put out virtual flyers to spread on-line to local hospitals, schools and internet sites and blogs. E-mails, IM's and networked text and voice messages were sent out. Because we (police) do not yet have a system in place, we were out of the loop. The TV media soon called us after a few days of this cyber-world investigation, asking us for comment on the investigation. We didn't know anything about it, so I tapped in. I was shocked to see all of the community interaction on what we considered a common police report that was quickly filed away. That caused us to get up to speed and go onto local TV stations to assure the public we were on the case (sort of). Lesson learned. (M. Stigler, personal communication, July 30, 2010)

B. CASE STUDY: FUSION CENTER

The second case study involved Aaron Kustermann, Chief Intelligence Officer for the Illinois State Police. Kustermann oversees all intelligence collection and response operations for the Illinois fusion center, known as the Statewide Terrorism and Intelligence Center (STIC), as well as field intelligence personnel.

The Illinois fusion center has made several proposals recently in an effort to research the next evolution of intelligence functions. Kustermann's office has been exploring Twitter accounts to test viability for open source, non-FOUO material to liaise with emergency managers, such as volunteer firemen. Their goal is to increase communications from the fusion center to the first-responder population to promote real-time communications and transfer of data. When it comes to direct communications with citizens, however, Kustermann's fusion center takes a hands-off approach:

> We have a different philosophy than many other fusion centers. Many of them talk directly to the public, to individual citizens and take information directly from them. We do not. As part of our strategy, we rely on those closest to the public to talk to us. For instance, public safety officials, fire and emergency management are our integration point; we receive information from the local public safety unit of government. We have stayed away from talking directly to the public because doing so would alienate our first-responder partners. If a state-wide intelligence entity talks to the public, it leaves other entities, like the local police department, in the dark. (A. Kustermann, personal communication, August 18, 2010)

Kustermann is not entirely counting out communicating with the public; in fact, he believes that involving local citizens in the homeland security framework is a necessity. From his perspective, however, his fusion center is not the appropriate entity to do this:

> I do believe, however, that we could be the facilitation point. For instance, if we can develop a template to gather information and give that template to first responders and local law enforcement, we can help them create a platform to collaborate with citizens. We end up being the beneficiary. But we, as a fusion center, cannot be responsible for a discussion with 12 million people. Our objective is to get to the public; our mechanism might be to help others get to the public. (A. Kustermann, personal communication, August 18, 2010)

According to Kustermann the problem with using social media for direct liaison between fusion centers and citizens is that the fusion center is unable to take action if it receives information that requires an immediate response.

> We are not in a position to mitigate local real-time emergency situations. We have a massive relationship with the private sector, but we tell them, if you come to us with an incident first, you've made a mistake. Our fusion center should not handle 9-1-1 type situations; we are going to refer them back to the local unit of government. Otherwise, we will begin to deal with issues that members of the public think to be homeland security problems that really aren't. First vetting should be done by local law enforcement. There are many ways in which the government should be interacting with citizens, but it has to be done at a level that is appropriate: allow the local police to act as the local police, and leverage the fusion center's relationship with the local police to collect relevant information. We are better able to manage conversations that way. (A. Kustermann, personal communication, August 18, 2010)

Kustermann's opinion of fusion center social media usage (as a tool to converse with the public) comes from experience. STIC experimented with engaging with the citizens of Illinois via social media:

> When we attempted to [sustain a statewide social media conversation] in the past, we've learned a quick and valuable lesson. The information is too abundant to manage; with that many people you do not know your users or their level of reliability. If you attempt to sustain that level of conversation with that many people, you need to prepare for the consequences you might encounter. It was extremely difficult for our fusion center to have a rich discussion with the public utilizing social media. A couple of hours into our exercise, I realized how quickly these conversations can get out of hand. I recognize that citizens are the next rung in the organization, however, and we have to go where they go. But [the STIC] has to consider the various rungs of communication that are most advantageous for our fusion center to use. Our rung is the first responders and local law enforcement; we can only be as modern or as trendy [with social media usage] as they are comfortable. A communications strategy for a fusion center has to consider all circles of individuals [statewide, first responders, and the public at large]. Otherwise, an unsustainable model could be implemented. We can fail by trying to do too much; it could be our silver bullet. (A. Kustermann, personal communication, August 18, 2010)

C. CASE STUDY: PUBLIC SAFETY DEPARTMENT

The third case study was conducted with Colonel Keith Squires, Deputy Commissioner for the Utah Department of Public Safety (UDPS) and State Director of Homeland Security in Salt Lake City, Utah. Squires played a central role in the development of the Utah fusion center and is at the forefront of developing its social media policy.

Squires's department is currently utilizing social media technologies to liaise with first responders such as law enforcement and fire departments. "I have approved [social media] use by my public information officers, and we have purchased a system called PIER that we are currently implementing. The Utah Fusion Center's Public Information Officer (PIO) uses the system; it has a component that integrates with our website and allows us to push communication through various channels" (K. Squires, personal communication, August 18, 2010). According to the PIER Systems website, "PIER is intended to help government agencies keep stakeholders informed with the latest news and updates while providing access to critical information during crises such as hurricanes, floods, power outages, extreme weather conditions, security threats and more" (O'Brien's Response Management, 2010). Government subscribers to PIER, like the Utah Department of Public Safety, can post information to a web-based interface that other users can download and subscribe to RSS feeds. Users are able to post questions and get feedback using the system as well (O'Brien's Response Management, 2010). Squires noted that the PIER site was particularly useful during the Gulf oil spill incident as it enabled the real-time exchange of information and allowed users to push information out to many sources simultaneously (K. Squires, personal communication, August 18, 2009).

Squires agrees that social media has advantages when it comes to cross-communication:

> Both sharing information and receiving information from the public are advantageous, and it also allows us to reach sectors of the population that we would normally not have access to. Social media benefits us because it creates a networked environment that educates the public while at the

> same time provides real-time information and situational awareness to the public. It has also provided an economical way to communicate with a portion of our constituents. We can post general information, such as the DHS "See Something, Say Something" initiative and get the word out. (K. Squires, personal communication, August 18, 2009)

Although Squires maintains a positive view of social media, when it comes to pushing messages and information out to constituents, he does not think that Utah's fusion center should utilize social media for two-way interactions with the public.

> In our circumstance, the fusion center is an analysis agency, not a response agency. If a member of the public uses 9-1-1, for example, our design is such that we are plugged into those first responder entities through our intelligence liaison officer program, which has representatives who are trained to communicate on a daily and weekly basis with our fusion center. That is a much more appropriate use [of social media within the Utah fusion center]. If I were to receive [emergency information] through our agency, it would actually slow down the response process; in the time it would take to push that information back down to the local agencies, the dispatch center, and get an officer on the scene, we would actually be taking the information we received and be reporting it secondhand. Information coming directly to us from the public is not the most efficient way to respond to an incident. (K. Squires, personal communication, August 18, 2010)

Squires also notes that adopting social media usage for the purposes of citizen communication would take both time and resources that Utah's fusion center cannot feasibly allocate.

> Manpower is a key issue for us, with the economy the way it is, we've lost a couple key positions and we are struggling to do more with fewer people. One of the obstacles of using social media at a fusion center is the information that could potentially come in [from social media sites]. That kind of information would need to be monitored regularly to decide whether it is credible or not and to determine who to push it out to. I do not have the manpower or the resources to do that. (K. Squires, personal communication, August 18, 2010)

From Squires's point of view, the initial interest that public safety officials had in social media usage is beginning to taper off:

> In my area, social networking peaked about a year ago in the emergency management community and interest seems to be waning. Twitter was a popular social networking site, but does not seem to keep the sustained interest of its clients. Social networking in general is not mentioned much of late. My concern is that these sites do not seem to naturally attract large portions of the population, unless it is a hot issue that has received a great deal of public interest. Despite that, though, the Utah Department of Public Safety is very active in social media and uses it to talk to first responders. We just feel that using social media at the fusion center level would not be as effective, which is why I don't anticipate using the social media that exists today for that purpose (K. Squires, personal communication, August 18, 2010)

V. CASE STUDY ANALYSIS AND RESEARCH IMPLICATIONS

A. LAW ENFORCEMENT

The city of Waukesha's police department employs 154 officers and staff members. Although Stigler was originally opposed to social media usage as a means to communicate with the public, he is now at the forefront for social media policy development for the city of Waukesha, which has a total of 550 city employees. His department is currently looking to develop a social media policy that could include a constituency of 700,000 people.

Stigler recognized that not only was social media a tool that could be used to leverage conversations with the residents of Waukesha, but the residents were, in essence, demanding that his department capitalize on these technologies and use them to aid in investigations in cases of kidnappings and abductions. The ability to communicate instantaneously to a broad audience can be a crucial; saving time may save lives. Stigler initially struggled to change attitudes within his department, but with the rise of social media popularity and citizen demand, Stigler was given the go-ahead to begin using social media to communicate with the public.

It appears as though many local law enforcement entities such as Stigler's are rapidly adopting social media policies to relay information to the public during citywide emergencies and to strengthen public/law enforcement relationships. For example, Ryan Loew describes the growing social media adoption trends throughout the country. "Municipalities across the country are adopting mobile and social media services to immediately broadcast emergency and community information. These new tools aren't replacing the tornado sirens and emergency broadcast systems—they're adding to them" (Loew, 2010). Tools such as Nixle aid in the effort to push out notifications to constituents during emergencies or other events that could potentially impact the community. Getting crisis communications to residents is not the only benefit for local governments when engaging in social media. "A quick search of Facebook and Twitter yields a host of government entities actively posting about official business, and not just

emergencies. Social media sites can now connect users with information about city council meetings, trash pickup, and road construction." Stigler noted these uses and more during his interview.

Because Stigler can remember a time when cell phones were a luxury, he recognizes that technology is growing, changing, and adapting at a rapid pace. He is already looking to the next generation of technology that the city of Waukesha and his department can use to better ensure the safety of the citizenry and to foster open dialogue between the public and the local government. He recognizes that there will be growing pains when adopting any sort of new technology and that personnel will have to be trained and retrained. In addition, cyber-security, privacy, and records retention concerns will have to be immediately addressed in order to protect the cyberinfrastructure of the city and remain in compliance with state laws on how to protect personally identifiable information posted by the public, as well as how to archive these electronic conversations.

B. FUSION CENTER

The Illinois fusion center, known as the Statewide Terrorism and Intelligence Center (STIC), employs 3,500 people and has a constituency of 12.9 million people. Kustermann's fusion center has been exploring social media usage via Twitter to engage in conversations with emergency managers throughout the state of Illinois. From Kustermann's point of view it is more practical and realistic to liaise with approximately 700 groups of first responders, volunteer firemen, and city law enforcement officials than it is to attempt to maintain social media accounts with the public that could potentially have millions of followers. Additionally, talking directly to the citizens of Illinois could potentially alienate first responders, which would slow down response times and risk missing vital pieces of intelligence due to an overabundance of incoming information from the public. When the STIC attempted to conduct a conversation using social media with the citizens of Illinois, they found after a short period of time that the overwhelming amounts of information proved to be too much to delve through, rendering the conversation unsustainable. From his experience, the STIC's usage of social media is

better utilized to engage with the first responder community and allow those first responders to use whatever social media tools they have available to communicate with their citywide constituencies.

Kustermann sees the future of social media platforms as an ever-changing phenomenon and does not count out the possibility of liaising, on some level, with the public in the future:

> There may be technological solutions ahead; people are trying to figure this problem [capturing and utilizing the information present in social media to strengthen homeland security]. The future may hold software that marries all of these social media tools into something that can aggregate the answers. We have to get where the suspicious activity is occurring and this will only happen if homeland security professionals communicate with the public on some level. (A. Kustermann, personal communication, August 18, 2010)

C. PUBLIC SAFETY DEPARTMENT

The Utah Department of Public Safety (UDPS) in Salt Lake City currently has 1411 total employees, of which 522 are sworn police officers. Squires, being a key player in the establishment of Utah's fusion center, is also responsible for the adaptation of its social media policy. Squires has since approved the purchase of PIER, which is a system designed to post information to appropriate personnel in the event of an emergency. Squires believes that social media is an inexpensive mechanism for Utah's Public Safety Department to reach the public; however, he does not believe that fostering two-way communication between Utah's 2.8 million citizens and the department is currently feasible. In Squires's view, the fusion center is an intelligence agency, not a first responder. Like Kustermann, Squires believes that fusion centers using social media to create two-way relationships with the public could potentially do more harm than good by cutting out public communication with local law enforcement and emergency managers and creating a lag in response times.

Additionally, due to recent cutbacks, Utah's fusion center does not have the budget to allocate resources to maintain social media usage with a statewide network, especially when, from Squires' point of view, public interest in communicating with the government via social media has peaked and waned.

Despite the perceived tapering off of Utah's public interest in a dialogue with its government, the Utah state government remains at the forefront of social media integration. In August 2010, the state of Utah was recognized for its social media integration efforts by being awarded the title of "Best Fit Integrator" by the Center for Digital Government (Enhanced Online News, 2010).

D. CROSS-CASE ANALYSIS AND RESEARCH IMPLICATIONS

As the case studies illustrate, there are various implementation issues associated with the use of social networking technologies within fusion centers as well as the homeland security and law enforcement framework. Lack of resources is one of the main deterrents when departments and agencies (be they local law enforcement, fusion center, or public safety) examine the possibility of using social media. Because the success of social media, from a homeland security perspective, hinges on real-time updates that contain vetted, accurate information, case study participants cited the potential need for additional personnel in order to adequately maintain social media sites within their agencies. Obtaining the buy-in of leadership and training officers and staff on the appropriate usage of social media will consume additional time and resources; senior staffers and department leaders may not have entered a workforce with Web 2.0 capabilities and may not recognize the potential benefits of adopting new (and potentially costly) methods of communicating with the public.

Case study participants have encountered various privacy and administrative law issues as they attempt to integrate Web 2.0 technologies and social media into their everyday operations. As social media has become a part of the federal, state, and local government framework, privacy concerns have arisen in the media and within privacy offices nationwide. Fusion centers are under particular scrutiny by privacy officials, as their mandate requires that they examine the activities of U.S. citizens. DHS in particular

has conducted privacy-impact assessments and subsequent privacy compliance verifications for state-operated fusion centers. These compliance measures have had a resonating effect; case study participants recognize that, particularly at the outset, the integration of social media technologies will require regular privacy and other administrative law training for their agency personnel. These other administrative law concerns, such as record keeping requirements and FOIA, are being addressed by entities like GAO and will remain a primary concern as social media is adopted within federal, state, and local entities in the future.

Additionally, case study participants agreed that they anticipate increased cyber-security concerns as they attempt to utilize Web 2.0 technologies to liaise with first responders, local law enforcement, and/or the public. The growing need to protect America's cyberinfrastructure is evident and the Obama administration, Congress, and DHS continue to push for both cybersecurity awareness and the implementation of cybersafeguards within federal, state, and local agencies, as well as the private sector. As social media continues to evolve, any new applications being used by homeland security and law enforcement personnel to create relationships within local communities will need to be evaluated in order to protect them from cyberattack.

Despite these potential problems the question remains: how can state-operated fusion centers, in conjunction with local law enforcement agencies, utilize social networking technologies in order to strengthen their relationship with citizens within their communities and subsequently strengthen homeland security efforts? There is no debate that social media has grown over the past year at a staggering rate and has infiltrated every aspect of American society. Fusion centers and local law enforcement personnel are increasingly aware of this growth and have experienced a need to shift in order to adapt to Web 2.0 technologies. Despite the rapid growth of Web 2.0, however, the fusion center and public safety case study participants agree: although social media is a rapidly growing phenomenon, utilizing it within an agency whose mandate is intelligence gathering may actually hinder response times in the event of an emergency, terrorism-related or otherwise. Social networking technologies, in their current form, may *not* be the solution to bridge existing gaps between the public and fusion centers. Maintaining an

ongoing virtual dialogue with thousands, or even millions, of constituents may not be a feasible solution to bridging the gap between fusion centers and their statewide constituency. Both the fusion center and the public safety case study participants agreed that local law enforcement, fire, and emergency responders are better equipped to leverage two-way conversations with the public and are better able to manage incoming data from social media. Because they likely deal with fewer constituents, local law enforcement may be able to better identify and vet information gathered from citizens. The fusion center and public safety participants also agreed that having direct conversations with the public at large could potentially hinder fusion center and public safety communications with their first-responder partners. In their view, social media would serve a more useful purpose for fusion centers if it were a means to share information with the local law enforcement entities in individual cities. In other words, city and county personnel should engage their citizenry, and statewide entities such as fusion centers and state public safety departments should engage with city and county personnel. From a local law enforcement perspective, social media usage may reduce future public need as the ability to push information to citizens on a real-time basis may result in the reduction of calls during both emergencies and non-emergencies. Conversely, being able to receive information from the public via social media could, in effect, result in faster law enforcement personnel response times and promote stronger relationships between officers and citizens.

In the homeland security environment the use of social media offers both new capabilities and challenges. An assessment of the three organizations contained in this thesis showed that, despite the fact that social media in its current iteration may not be the best platform to sustain relationships between fusion centers and citizens, case study participants agreed that social media technologies will continue to grow and adapt to the needs of users. Because of the numerous potential benefits that social media integration could have on homeland security efforts, none of the case study participants in this thesis counted out future use of social media technologies within their agencies as a successful tool for liaising with the public. In the future, there may be federal and state standards implemented across agencies as the ongoing discussion about the potential uses of social

media continues. Whether these standards will become congressionally mandated, passed down by agencies such as DHS, or kept at a local level is currently unknown. However, one thing remains certain: social media will inevitably impact homeland security efforts and will shape the role in which the public participates in that effort.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSION

A. DISCUSSION

The Obama administration's efforts to integrate social media into all levels of government appear to be taking hold with the American public. According to Nextgov, "Citizen satisfaction with federal Web sites increased significantly in 2009, indicating efforts by the Obama administration to increase transparency in government are getting noticed, according to a new report [released by ForeSeeResults]" (Aitoro, 2010,). The recent push on behalf of the federal government to incorporate social media into its daily operations has begun to translate into the homeland security realm and within such agencies as Federal Emergency Management Agency (FEMA). As the FEMA listserv recently touted, Administrator Craig Fugate "has made a concerted effort to engage the private sector as part of the nation's emergency management team. He has made the use of social networking sites and other new media a central component of the agency's public outreach" (e-mail communication to author).

Studies conducted on social media usage by American citizens suggest that social media has exposed a broader citizen population wishing to be informed by its government. USA Government Online Reports, "Moreover, these new [social media] tools show particular appeal to groups that have historically lagged in their use of other online government offerings—in particular, minority Americans. Latinos and African Americans are just as likely as whites to use these tools to keep up with government, and are much more likely to agree that government outreach using these channels makes government more accessible and helps people stay more informed about what government agencies are doing" (INFORUM, 2010). If poll statistics are an indicator, a broad demographic of citizens would take advantage of the opportunity to use social media as a mechanism to receive information from and/or participate in government operations if given the option. "According to a recent 2010 Federal Community Social

Media study by Market Connections, 55% of respondents are using social media either formally or informally to communicate with their government audiences" (Radick, 2010, p. 2).

The reality is that social media has begun to affect everyone, even those citizens who initially chose not to use it for personal or professional purposes. Those who don't engage in social media lack the advantage of receiving information on a real-time basis, although some may say that disengagement is a blessing and that a constant stream of information is unnecessary and burdensome. Disengagement, however, may have its disadvantages, particularly with the growing attention that social media has received within the local law enforcement and first responder communities. Citizens engaged in social media have the capability to receive more timely information from their government, first responder, and/or local law enforcement entities in future emergency situations. Recent online articles illustrating the growing use of social media as a mechanism for the government to communicate with the public are abundant and published on a near-daily basis. For example, the Environmental Protection Agency (EPA) used Twitter and Facebook to share information with citizens during the Gulf oil spill in 2010. FEMA, Virginia's Department of Emergency Management (VDEM), and the National Weather Service, all of which have used Twitter to send messages and emergency communications to citizens, have also been highlighted ("Social Media Helps US Government Interact Better with Officials and Citizens," 2010).

B. THE WAY FORWARD

1. Fusion Centers

Because each fusion center is unique and structured to a state's specific needs, fusion centers should assess their capabilities to determine what avenues social media can provide to assist them in connecting to their local community (be it citizens or first responders). Each individual fusion center should retain its autonomy and ability to determine what technologies best fit its needs. Even if current social media do not provide the adequate controls and aggregation tools necessary to be an effective tool for

communicating with the public, fusion centers should not count out future social media use entirely. As with most technology, social media will likely continue to evolve to adapt to the growing needs of its users. If one isn't already in place, fusion centers should develop a plan to allocate future resources to ensure that, when the right social media fit comes along, they are prepared to integrate the technology. Additionally, fusion centers need to formulate strategic plans to obtain adequate personnel and prepare to train center staff on new media as it arises. Although federal fusion center guidelines could be updated to reflect the growing national interest in social media and its privacy, administrative law, and cybersecurity implications, there should be no overarching mandate placed on the fusion center framework as a whole to adopt a particular social media platform. Doing so could be cumbersome and may hinder social media adoption practices more than abate them.

Fusion centers should also examine their daily operations to assess whether social media could serve as a tool to communicate with state and local law enforcement and first responder communities. The real-time nature of social media such as Twitter and Facebook could potentially provide additional situational awareness between various homeland security entities and result in faster response times during emergencies. Collaboration and communication also helps foster important relationships between separate but related homeland security communities, a key element to the overall safeguarding of citizens, communities, and the nation's critical infrastructure.

2. Law Enforcement Agencies

Law enforcement agencies may be better positioned to utilize social media (in its current form) within their departments to foster citizen engagement. Although there has been a push within various city governments to adopt social media policies and best practices for local police departments, many are still learning. In their 2010 publication, the International Association of Chiefs of Police (IACP) Homeland Security Committee focused on a strategy to continue to incorporate social media into daily law enforcement operations. The IACP notes that harnessing social media technologies may be a key element to the sharing of crucial information: "To truly develop a police culture that can

exchange data, information, and intelligence to interpret the criminal environment and address occurring threats and hazards in near real time, broad changes to the way law enforcement organizations manage their information must occur. Although there is still much room for improvement with social media technologies … law enforcement can learn a great deal from their current applications" (IACP, 2010, p. 5).

C. CONCLUSION

Although the fusion center, public safety department, and local law enforcement case studies help illustrate the various social media practices of entities that have a myriad of homeland security responsibilities and constituency bases, there are limits to the case study method of research. While the case studies provide an in-depth account of the specific social media practices of three agencies, there is much more to explore in the way of social media integration into the fusion center and law enforcement framework as a whole. The case studies are not indicative of the policies and practices of all fusion centers, public safety departments, and law enforcement agencies. Furthermore, there may be no "one size fits all" solution for every homeland security agency when attempting to integrate social media in a way that is useful and beneficial to the homeland security mission insofar as it relates to involving American citizens in homeland security operations. As was illustrated in all three case studies as well as in the literature review, there are several hurdles that homeland security entities will encounter when entering into the social media realm. There are many federal laws that need to be adhered to when engaging with the public. Privacy and other administrative law issues such as record keeping are a concern within federal privacy and record keeping offices (particularly when dealing with fusion centers), and cybersecurity is a rapidly changing phenomenon that requires adequate and regularly updated safety measures to ensure the protection of an agency's cyberinfrastructure. Research on these topics is generated on a regular basis and will continue to change how Web 2.0 technologies can be safely integrated within fusion centers and local law enforcement agencies and remain in compliance with the law. And because articles containing new research and findings on Web 2.0, social

media, fusion centers, privacy and record keeping matters, and cybersecurity are produced on an ongoing basis, an entire set of theses on these various topics can (and should) be published in the future.

Based on the case study findings, social media in its current iteration may not be the right fit for fusion center/citizen engagement. The sheer size of some of the constituency bases with which certain statewide entities would be trying to engage might solicit an overinflux of information that could render the engagement ineffective. Some local law enforcement entities may have a better knowledge-base of their citizenry and deal with a smaller percentage of the population than would a state-operated fusion center. For example, cities such as Waukesha with smaller populations may have an easier time leveraging conversations with its citizens via social media and can work to develop a trusted set of citizen liaisons.

Due to an ever-changing homeland security environment, social media adaptation by fusion centers for purposes of community interaction may be inevitable, regardless of the number of citizens who reside in a particular state. If millions of people are using social media to communicate, homeland security professionals need to take a proactive approach, tap into that resource, and adapt to exist within the parameters of interaction that American citizens have chosen. Despite potential privacy, record keeping, or cybersecurity issues, Web 2.0 and social media will eventually change the face of every homeland security entity. The push by the Obama administration for a more transparent, citizen-centric government has created a new way of thinking among federal, state, and local governments, and citizen participation has become a mainstay of newly written policies across the country. “The reinvention of government breaks down silos, improves citizen service and opens up the possibilities of collaboration and broader participation among agencies and by citizens themselves. In effect, Web 2.0 represents another step in the inexorable move to more citizen-centric and participatory government” (Accenture, 2009, p. 8).

Taking the first steps to adopt social media technologies may be difficult for fusion centers and local law enforcement entities in the beginning, but over time the potential benefits of citizen collaboration greatly outweigh initial integration challenges.

The use of social media within state-operated fusion centers and local law enforcement will allow for collaboration among homeland security entities, first responders, law enforcement, and local citizens. This sort of collaboration could result in a stronger homeland security community and a general sense of resonating responsibility throughout the American population.

There is no matrix or way to gauge the potential impact that collaborative relationships between citizens and the homeland security community will have on strengthening the security of the nation. Many of the potential outcomes are hypothetical and are based on circumstantial situations where there is no real way to assess the outcome or impact. What is certain, however, is that the more American citizens are engaged in homeland security efforts, the better the chances of thwarting a potential terrorist plot. As terrorists continue to grow smarter, attempt to gain access to the critical infrastructure of the United States, and use any means necessary to cause harm, the first line of defense is the average American citizen who is far more likely to witness suspicious or potential terrorist activities before that of a homeland security or law enforcement official. Community involvement in homeland security can be fostered through the use of social media tools; homeland security and local law enforcement professionals should provide an avenue for the public to participate and share what could be vital, life-saving information.

APPENDIX

Research Question: How can state-operated fusion centers integrate social networking technologies into daily operations to more effectively collaborate with their local citizens and strengthen the homeland security mission to mitigate the threat of terrorism?

Interview Questions:

1. What is your familiarity with social media?
   1.1. As related your current position?
   1.2. As related to your personal interest (in sum, is the interviewee familiar with the numerous no/low cost social medial tools being used)?
   1.3. What has your involvement been (if any) with social media implementation in your department/agency?
2. Has your organization discussed or considered the use of social media tools to support its mission?
3. What would be the objective of use of social networking platform(s)? Sharing info with the public and/or receiving info from the public?
4. What are some of the implementation issues you encountered/are encountering with social media adaptation in your department/agency?
   4.1. What do you see as the potential benefits of social media adaptation at your department/agency?
   4.2. What are some potential drawbacks of using social media to collect information and collaborate with local citizens within the fusion center framework?
5. How do you think social networking technologies can create bridges of communication between the public and fusion centers?
   5.1. How have social media technologies worked in practice at your department/agency so far? Are you aware of others entities in your department, state, county, etc. using or considering the use of social media to support ongoing or anticipated activities? What lessons learned have they offered?

5.2. How have social media technologies influenced your department/agency's relationship with local citizens?

5.3. Do you have any success stories you can share?

5.4. Do you have any challenges, failures, concerns, related stories you can share?

5.5. Do you have any lessons learned you can share?

6. How do DHS policy and fusion center guidelines affect the daily operations of your department/agency?

6.1. In your opinion, how will DHS policy and fusion center guidelines need to be modified in order to accommodate and support the introduction of social networking sites into everyday HLS operations?

7. In your opinion, how will social media affect the relationship that HLS officials have with local citizens in the future?
8. Who in your organization would need to participate in and be a part of the review process prior to a social networking tool being used in the fusion center? (lawyers, resource managers, privacy/civil liberty, FOIA staff, law enforcement officials, etc.
9. If social media were to be introduced into your department/agency, what type of training might be required of management and staff?
10. What types of information would your department/agency place on the social networking platform? What types of information would be omitted from the platform?
11. How would your department/agency safeguard against citizens using the platform to place malicious information about others that could in turn cause law enforcement to follow bogus leads? Would penalties be incurred by individuals intentionally misusing the system (i.e., much like hoax 911 calls)?
12. How would your department/agency determine the credibility and viability of information posted by a citizen on the platform?

LIST OF REFERENCES

Accenture. (2009). Web 2.0 and the next generation of public service: Driving high performance through more engaging, accountable and citizen-focused service. Retrieved December 8, 2010, from http://www.accenture.com/NR/rdonlyres/C70B1B86-E876-4A20-9CF1-5121ABB2668A/0/Accenture_Public_Service_Web_2_dot_0_in_Public_Service_3.pdf

Aitoro, J. R. (2010). Public satisfaction with federal Web sites increased in 2009. Retrieved March 11, 2010, from http://www.nextgov.com/site_services/print_article.php?StoryID=ng_20100126_3700

Bach, R., & Kaufman, D. J. (2009). A social infrastructure for hometown security: Advancing the homeland security paradigm. *Homeland Security Affairs Journal* 5(2), 1–13. Retrieved December 8, 2010, from http://www.hsaj.org/?article=5.2.2

Bunt, G. (2008). Controlling access for social networking. *Malayasian Business*. Retrieved December 8, 2010, from http://findarticles.com/p/articles/mi_qn6207/is_20080916/ai_n28113725/

Carafano, J. (2009). Social networking and national security: How to harness Web 2.0 to protect the country (Backgrounder No. 2273). Washington, D.C.: Heritage Foundation. Retrieved December 8, 2010, from http://s3.amazonaws.com/thf_media/2009/pdf/bg2273.pdf

CIO Council. (2009). Guidelines for secure use of social media by federal departments and agencies. Washington, D.C.: CIO Council. Retrieved December 8, 2010, from http://www.cio.gov/Documents/Guidelines_for_Secure_Use_Social_Media_v01-0.pdf

Currie, D., Tinker, T., & Fouse, D. (n.d.). Special report: Expert round table on social media and risk communication during times of crisis: Strategic challenges and opportunities. Washington, D.C.: American Public Health Association. Retrieved December 8, 2010, from http://www.apha.org/NR/rdonlyres/47910BED-3371-46B3-85C2-67EFB80D88F8/0/socialmedreport.pdf

Cyber-Security survey shows distrust between public and private sectors. (2010). Government Technology. Retrieved December 8, 2010, from http://www.govtech.com/gt/759431

Drapeau, M., & Wells, L., II. (2009). Social software and national security: An initial net assessment. Washington, D.C.: Center for Technology and National Security Policy, National Defense University. Retrieved August 10, 2009, from http://www.ndu.edu/CTNSP/docUploaded/DTP61_SocialSoftwareandNationalSecurity.pdf

Electronic Privacy Information Center. (2010). Information fusion centers and privacy. Retrieved August 16, 2010, from http://epic.org/privacy/fusion/

Enhanced Online News. (2010). Utah.gov wins national award for social media efforts. Retrieved August 18, 2010, from http://eon.businesswire.com/portal/site/eon/permalink/?ndmViewId=news_view&newsId=20100818005368&newsLang=en

Facebook. (2010). User statistics. Retrieved December 1, 2010, from http://www.facebook.com/press/info.php?statistics

Federal Web Managers Council. (2008). Social media and the federal government: Perceived and real barriers and potential solutions. Washington, D.C.: Federal Web Managers Council. Retrieved December 8, 2010, from http://www.usa.gov/webcontent/documents/SocialMediaFed%20Govt_BarriersPotentialSolutions.pdf

Gerencser, M. (2008). Megacommunities: How leaders of government, business and non-profits can tackle today's global challenges together. New York: Palgrave Macmillan.

Godwin, B., Campbell, S., Levy, J., & Bounds, J. (2008). Government and social media. Paper presented at the Social Media for Communicators Conference. Retrieved December 8, 2010, from http://www.usa.gov/webcontent/documents/Government_and_Social_Media.pdf

Granger, S. (2002). Social engineering fundamentals, part 2: Combat strategies. Retrieved September 3, 2010, from http://www.symantec.com/connect/articles/social-engineering-fundamentals-part-ii-combat-strategies

Homeland Security Policy Institute. (2009). Cyber Deterrence Symposium. George Washington University, Washington, D.C. Retrieved November 2, 2009, from http://www.gwumc.edu/hspi/events/CyberSymposium.cfm

Hrdinova, J., Helbig, N., & Peters, C. S. (2010). Designing social media policy for government: Eight essential elements. Albany, NY: Center for Technology in Government, SUNY at Albany. Retrieved December 8, 2010, from http://www.ctg.albany.edu/publications/guides/social_media_policy/social_media_policy.pdf

INFORUM: Forum of Hungarian IT organizations for information society. (2010). USA: Government Online. Retrieved May 5, 2010, from http://einclusion.hu/2010-05-02/usa-government-online/

International Association of Chiefs of Police. Homeland Security Committee. (2010). Razing expectations: Erecting a strategic vision for fusion centers. Alexandria, VA: International Association of Chiefs of Police. Retrieved December 8, 2010, from http://www.theiacp.org/LinkClick.aspx?fileticket=A%2b72iBFNpLw%3d&tabid=87

Internet.com.Web 2.0 Online Definition. (n.d.). Retrieved August 20, 2009, from http://www.webopedia.com/TERM/W/Web_2_point_0.html

Kim, W. C., & Mauborgne, R. (2005). Blue ocean strategy: How to create uncontested market space and make the competition irrelevant. Boston, MA: Harvard Business School Press.

Kingsley, C. (2010). Making the most of social media: 7 lessons from successful cities. Philadelphia, PA: Fels Institute of Government, University of Pennsylvania. Retrieved December 8, 2010, from https://www.fels.upenn.edu/sites/www.fels.upenn.edu/files/PP3_SocialMedia.pdf

Kubota, S. (2009). DHS listens and learns at Ogma. FederalNewsRadio.Com. Retrieved December 8, 2010, from http://www.federalnewsradio.com/index.php?nid=110&sid=1719126

Loew, R. (2010). Municipalities use social media to bridge communication gap. Lansing State Journal. Retrieved July 25, 2010, from http://www.lansingstatejournal.com/article/20100725/NEWS01/7250494/Municipalities-use-social-media-to-bridge-communication-gap&template=artsemantics&server=MOC-WN0336

McCullagh, D. (2010). Pentagon, State Department OK social-network use. Cnet.News Digital Media. Retrieved December 8, 2010, from http://news.cnet.com/8301-1023_3-20010409-93.html

O'Brien's Response Management. (2010). PIER systems: Government. Retrieved August 18, 2010, from http://www.piersystems.com/go/doc/1533/260628/

Oregon Department of Administrative Services. (2010). Social networking media: Combining technology and social interaction to create value. Salem, OR. Retrieved December 8, 2010, from http://www.oregon.gov/DAS/EISPD/EGOV/BOARD/docs/social_networking_guide_v1.pdf

O'Reilly, T. (2010). Opening the doors of government to innovation. Retrieved August 7, 2010, from http://radar.oreilly.com/2010/08/opening-doors-government-innovation.html

Radick, S. (2010). How social media is changing the way government does business. Retrieved July 16, 2010, from http://mashable.com/2010/07/02/social-media-government-business/

Riegle R. (2009). The Future of Fusion Centers: Potential Promise and Dangers. Testimony of Director Robert Riegle, State and Local Program Office, Office of Intelligence and Analysis, before the Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment. Washington, D.C.: Department of Homeland Security. Retrieved July 25, 2009, from http://www.dhs.gov/ynews/testimony/testimony_1238597287040.shtm

Rollins, J., & Henning, A. C. (2009). Comprehensive national cybersecurity initiative: Legal authorities and policy considerations (No. R40427). Washington, D.C.: Congressional Research Service. Retrieved December 8, 2010, from http://www.fas.org/sgp/crs/natsec/R40427.pdf

Rollins, J., & Wilson, C. (2007). Terrorist capabilities for cyberattack: Overview and policy issues (No. RL33123). Washington, D.C.: Congressional Research Service. Retrieved December 8, 2010, from http://www.fas.org/sgp/crs/terror/RL33123.pdf

Sadeh, N., Hong, J., Cranor, L., Fette, I., Kelley, P., Prabaker, M., & Rao, J. (2007). Understanding and capturing people's privacy policies in a mobile social networking application. *Personal and Ubiquitious Computing* 13(6), 401–12.

Short, J. (2008). Risks in a Web 2.0 world. *Risk Management* 55(10), 28–31.

Social media helps US government interact better with officials and citizens. (2010). Retrieved May 20, 2010, from http://www.onesocialmedia.com/blog/2010/05/social-media-helps-us-government-interact-better-with-officials-and-citizens/

Solove, D. J. (2008). *Understanding privacy*. Cambridge, MA: Harvard University Press.

Sullivan, J. (2009). Harnessing open source intelligence: Social media and the CIA. FindingDulcinea. Retrieved December 8, 2010, from http://www.findingdulcinea.com/news/Americas/2009/October/Harnessing-Open-Source-Intelligence--Social-Media-and-the-CIA.html

Theohary, C. A., & Rollins, J. (2009). Cybersecurity: Current legislation, executive branch initiatives, and options for Congress (No. R40836). Washington, D.C.: Congressional Research Service. Retrieved December 8, 2010, from http://www.fas.org/sgp/crs/natsec/R40836.pdf

United States Department of Homeland Security. (2008a). Civil liberties impact assessment for the state, local, and regional fusion center initiative. Washington, D.C. Retrieved December 8, 2010, from http://www.dhs.gov/xlibrary/assets/crcl_civil_liberties_impact_assessment_12_11_08.pdf

United States Department of Homeland Security. (2008b). Privacy impact assessment for the Department of Security state, local, and regional fusion center initiative. Washington, D.C.: Department of State. Retrieved December 8, 2010, from http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ia_slrfci.pdf

United States Department of Homeland Security. (2009). Government 2.0: Privacy and best practices report on the DHS Privacy Office public workshop, June 22 and 23, 2009. Washington, D.C.: DHS Privacy Office. Retrieved December 8, 2010, from http://www.dhs.gov/xlibrary/assets/privacy/privacy_rpt_govt20_2009.pdf

United States Department of Homeland Security. (2010). Privacy impact assessment for the operations coordination and planning: Haiti social media disaster monitoring initiative. Washington, D.C.: Department of Homeland Security. Retrieved December 8, 2010, from http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ops_haiti.pdf

United States Department of Justice. (2008). Privacy and civil liberties policy development guide and implementation templates. Washington, D.C.: Department of Justice's Global Justice Information Sharing Initiative. Retrieved July 25, 2009, from http://www.it.ojp.gov/documents/Privacy_Guide_Final.pdf

United States Department of Justice. (2010). Privacy, civil rights, and civil liberties compliance verification for the intelligence enterprise. Washington, D.C.: Department of Justice's Global Justice Information Sharing Initiative. Retrieved December 8, 2010, from http://www.ncirc.gov/documents/public/supplementaries/privacy_verification.pdf

United States Department of Justice and United States Department of Homeland Security. (2006). Fusion center guidelines: Developing and sharing information and intelligence in a new era. Washington, D.C.: Dept. of Justice Programs, Bureau of Justice Assistance. Retrieved July 25, 2009, from http://www.it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf

Van Leuven, L. J. (2009). Optimizing citizen engagement during emergencies through use of Web 2.0 technologies. Master's thesis, Naval Postgraduate School, Monterey, CA. Retrieved December 8, 2010, from http://edocs.nps.edu/npspubs/scholarly/theses/2009/Mar/09Mar_Van_Leuven.pdf

Werner, A. R. (2008). The Potential Transformation Impact of Web 2.0 Technology on the Intelligence Community. Master's thesis, Naval Postgraduate School, Monterey, CA. Retrieved December 8, 2010, from http://edocs.nps.edu/npspubs/scholarly/theses/2008/Dec/08Dec_Werner.pdf

White House. (2010). Retrieved September 9, 2010, from http://www.whitehouse.gov

White House Blog. (2009). New technologies and participation. Retrieved September 9, 2010, from http://www.whitehouse.gov/blog/New-Technologies-and-Participation/

Wilshusen, G. (2010a). The good and the bad of Fed Web 2.0. FederalNewsRadio.Com. Retrieved December 8, 2010, from http://www.federalnewsradio.com/?sid=2015017&nid=150

Wilshusen, G. C. (2010b). Information management: Challenges in federal agencies' use of Web 2.0 technologies (Testimony No. GAO-10-872T). Washington, D.C.: Government Accountability Office.

Woodcock, J. (2009). Leveraging social media to engage the public in homeland security. Master's thesis, Naval Postgraduate School, Monterey, CA. Retrieved December 8, 2010, from http://edocs.nps.edu/npspubs/scholarly/theses/2009/Sep/09Sep_Woodcock.pdf

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California